x-tention zeigte bewährte Cybersecurity-Lösungen an der IoT Security Konferenz und der InfoSec Health Konferenz in Cham

Wer Gefahren gezielt vorbeugt, zeigt Verantwortung für Betrieb und Patienten

Mehr als ein Cyberangriff pro Minute: Dieser Gefahr sind IT-Systeme heute ausgesetzt. Es braucht daher dringend modernste Sicherheitslösungen, um im Ernstfall schnell und effektiv zu reagieren. Noch besser wirkt Vorbeugen, damit die Risiken zum Vornherein minimiert werden können. Investitionen in die Cybersecurity sind gerade im Gesundheitswesen, wo besonders viele sensible Daten vorhanden sind, Gold wert.

Die zunehmende Vernetzung von IoT und IoMT-Geräten bringt erhebliche Sicherheitsrisiken mit sich – insbesondere in kritischen Infrastrukturen wie Spitälern. Peter Brillinger, Leiter des x-tention Cybersecurity Competence Centers, zeigte in einem ersten Vortrag in Cham praxisorientierte Lösungen zur Risikobewertung und reduktion, die es ermöglichen, Schwachstellen frühzeitig zu identifizieren und gezielt Gegenmassnahmen zu ergreifen. Anhand konkreter Anwendungsfälle demonstrierte er, wie Unternehmen ihre IoT-Sicherheitsstrategien optimieren und Bedrohungen proaktiv minimieren können.

Im zweiten gleichentags stattfindenden Anlass, der InfoSec Health Konferenz, ging es um «Healthcare Native Security für Spitäler». Peter Brillinger wies hier auf die besonderen Herausforderungen für die IT-Sicherheit hin, die beim Einsatz medizintechnischer Geräte entstehen. Herkömmliche Security-Lösungen decken oft nicht alle Bereiche ab. Dieser Vortrag des Experten deckte bisher wenig beachtete Sicherheitslücken im MedTech-Umfeld auf und zeigte spezifische Schwachstellen in der Spital-IT. Anschliessend wurde ein innovativer Ansatz vorgestellt, der diese Bedrohungen gezielt

Peter Brillinger, Leiter des x-tention Cybersecurity Competence Centers, zeigte in Cham, wie Cyberkriminalität wirksam vorgebeugt werden kann.

adressiert und das Sicherheitsniveau in Spitälern nachhaltig erhöhen kann. Praxisnahe Beispiele veranschaulichten schliesslich, wie eine «Healthcare Native Security» Strategie umgesetzt werden kann, um Patienten, Daten und Systeme effektiv zu schützen.

Gesundheitsdaten sind ein attraktives Ziel für Cyberkriminelle

Und guter Schutz ist unabdingbar, denn die Angriffe von Hackern nehmen zu. Derartige kriminelle Handlungen sind zu einem eigentlichen Geschäftsmodell geworden, das weltweit riesige Umsätze aus Erpressung von Lösegeldern erzielt. Gesundheitsdaten stellen dabei ein Ziel für Angreifer dar, und etliche Kliniken haben schon schmerzlich erfahren, wie administrative und medizinische Prozesse durch einen Cybervorfall lahmgelegt worden sind, ganz zu schweigen vom Reputationsverlust der betroffenen Spitäler. Persönliche, medizinische und finanzielle Daten sind eben unglaublich wertvoll. Daher ist die Versuchung gross, sie für Attacken zu nutzen. Die Angriffe erfolgen dabei, so Peter Brillinger, hauptsächlich über Phishing, die Ausnutzung von technischen Schwachstellen, die Verwendung von gestohlenen Zugangsdaten oder unsichere Konfigurationen.

Die Schäden sind meist erheblich. Untersuchungen, Eingriffe, Behandlungen oder Notfälle können nicht mehr durchgeführt werden. Es entstehen potenziell lebensbedrohliche Situationen. Die daraus entstehenden Belastungen sind Systemausfall, unversorgte Patienten, aufwändige Wiederherstellung von Systemen, und all das begleitet von nervenraubenden und teuren Verhandlungen.

Gesundheitseinrichtungen sind zudem recht vulnerabel, denn ihre IT ist mit medizinischer Infrastruktur kombiniert. Es bestehen spezielle medizinische Protokolle zwischen unterschiedlichen Geräten. Ausserdem sind viele Mitarbeitende, Kunden und Partner regelmässig mit verschiedenen Geräten involviert. Schliesslich erschwert auch die aktuelle Gesetzgebung rasche Updates bei Schwachstellen. Cybersecurity muss daher umfassend und systematisch betrieben werden.

Mit gründlichen Kontrollen fängt es an

Den Anfang einer gründlichen IT-Sicherheit stellen Kontrollen dar. Besonders beliebt sind endpunktbasierte Sicherheitskontrollen (z.B. EDR), netzwerkbasierte Sicherheitskontrollen (z.B. NDR) sowie Betriebs-/Überwachungskontrollen (z.B. SIEM) und bereichsübergreifende Sicherheitskontrollen (z.B. XDR). Geprüft werden können auch Identitäten, Daten, Clouds, Anwendungen, sowie die physische Sicherheit. Peter Brillinger: «Es muss eine Priorisierung von Systemen auch nach Patientensicherheit, nicht nur nach Geschäftswert erfolgen. Wichtig ist auch das Erkennen von spezifisch für Spitälern relevanten Angriffen, die normale SOCs eventuell übersehen würden (z.B. unautorisierte Nutzung von Medizingeräten oder Anomalien bei der Auslastung von Medizingeräten). Erfahrene Analysten kennen diese Spezifika im Gesundheitswesen und wissen Rat. Die Früherkennung von Angriffen sollte ein zentraler Baustein der Sicherheitsarchitektur jedes Spitals sein.»

Gezielter Aufbau der Cybersecurity

Peter Brillinger schilderte in seinem zweiten Vortrag eine häufige Ausgangslage: fehlende Sichtbarkeit im medizinischen Netzwerk, keine Mikrosegmentierung von IT-Systemen, fehlender medizinischer IT-Schwachstellenmanagement-Prozess und fehlende Früherkennung von Bedrohungen. Der Ansatz für eine gründliche IT-Sicherheit besteht hier in der Inventarisierung, Sichtbarmachung und Behebung vorhandener Schwachstellen, der Analyse möglicher weiterer Bedrohungen und deren Gefahrenpotenzial sowie der Modellierung potenzieller Risiken. Durch geeignete und bewährte Erkennungs- und Abwehrstrategien kann so die Wahrscheinlichkeit schwerwiegender Bedrohungen und Angriffe auf ein absolutes Minimum beschränkt werden.

Massnahmen auf Seiten der Betreiber sind Patches einspielen, eine Mikrosegmentierung implementieren, verwundbare/nicht verwendete Protokolle deaktivieren, persönliche Zugriffe einschränken und vom Nutzen eines Healthcare Native Security Operations Centers profitieren. MedTech-Hersteller sind ebenfalls gefordert. Ihre Hausaufgaben heissen regelmässige Updates und Patches bereitstellen, Schwachstellenscans und Penetrationstests bereits im Entwicklungsprozess durchführen, sowie Härtungsmassnahmen anwenden (Security by Design) und Secure Development Lifecycles etablieren.

Kompetent seit fast 25 Jahren

«Eine starke Cybersecurity zu schaffen und laufend auf dem neusten Stand zu halten – denn die Hacker werden immer raffinierter – ist eine Kernaufgabe eines Spitals. Und hier können wir einen entscheidenden Beitrag liefern», unterstrich Peter Brillinger. «Ein zentrales Angebot von x-tention ist das 24/7/365 Security Operations Center. Es überwacht kontinuierlich Sicherheitsereignisse, bewertet Risiken in Echtzeit und ergreift bei Bedarf sofortige Gegenmassnahmen. Ein persönlicher Security Technical Account Manager berät seine Kundinnen und Kunden zu allen Sicherheitsfragen – von SIEM & Threat Intelligence über Network & Endpoint Security bis zu Security Assessments & Penetration Testing. Sie/Er steht fortlaufend beratend zur Seite, informiert umfassend über die aktuelle Bedrohungslage und präsentiert die Ergebnisse präziser Angriffserkennung sowie den aktuellen Stand der Cybersecurity einer Gesundheitseinrichtung.»

Seit fast 25 Jahren harmonisiert und integriert die x-tention Unternehmensgruppe unterschiedliche IT-Systeme im Gesundheits- und Sozialwesen. An 16 Standorten unterstützen fast 800 Mitarbeitende mehr als 1000 Kunden erfolgreich in den Bereichen Consulting, Softwareentwicklung, Data Science, Delivery, Managed Services und Cybersecurity. Mit tief verwurzelter Healthcare-DNA, innovativen Technologien und höchster Liefertreue entwickelt x-tention massgeschneiderte Konzepte, um eine nachhaltige und zukunftssichere IT-Architektur zu gewährleisten. Die Lösungen verbessern die Patientenversorgung, steigern die Effizienz von Prozessen und sorgen für die sichere digitale Kommunikation zwischen den Akteuren im Gesundheitswesen.

Weitere Informationen

www.x-tention.com